STATE of ARIZONA

Government
Information
Technology
Agency

Statewide

STANDARD

P800-S855 Rev 1.0

TITLE: Incident Response and Reporting

Effective Date: April 5, 2004

1. AUTHORITY

The Government Information Technology Agency (GITA) shall develop, implement and maintain a coordinated statewide plan for information technology (IT) (A.R.S. § 41-3504(A (1))) including the adoption of statewide technical, coordination, and security standards (A.R.S. § 41-3504(A (1(a)))).

2. PURPOSE

This standard defines budget unit responsibilities for responding to and reporting cyber attacks and for sharing information related to potential incidents or threats with the State's Information Protection Center (SIPC).

3. SCOPE

This applies to all budget units. Budget unit is defined as a department, commission, board, institution or other agency of the state organization receiving, expending or disbursing state funds or incurring obligations of the state including the board of regents and the state board of directors for community colleges but excluding the universities under the jurisdiction of the board of regents and the community colleges under their respective jurisdictions and the legislative or judicial branches. A.R.S. § 41-3501(2).

The Budget Unit Chief Executive Officer (CEO), working in conjunction with the Budget Unit Chief Information Officer (CIO), shall be responsible for ensuring the effective implementation of Statewide Information Technology Policies, Standards, and Procedures (PSPs) within each budget unit.

4. STANDARD

To secure and protect the State of Arizona's critical IT business processes and assets from cyber-crime or cyber-terrorism, budget units shall report all cyber intrusions to the Statewide Information Protection Center (SIPC).

4.1. CYBER INTRUSIONS**:** Budget units shall report any of the following acts by any person who, **without authority** or **acting in excess of authority**:

- Accesses an IT device (server, storage, or client) or network with the intent to instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources of a computer, computer system, or network.
- Accesses, alters, damages, or destroys any IT device, network, or any physically or logically connected IT devices.
- Accesses, alters, damages, or destroys any computer application systems, programs, or data.

- Recklessly disrupts or causes the disruption of any services provided through the use of any IT device or network.
- Denies or causes the denial of IT-related services to any authorized user of those services.
- Recklessly uses an IT device or network to engage in a scheme or course of conduct that is directed toward another person and that seriously alarms, torments, threatens, or terrorizes the person.
- Prevents a computer user from exiting an Internet, Intranet, or internal host site, computer system, or network-connected location in order to compel the user's computer to continue communicating with, connecting to, or displaying the content of the service, site, or system.
- Knowingly obtains any information that is required by law to be kept confidential or any records that are not classified as public records by accessing an IT device or network that is operated by the State, a political subdivision of the State, or a medical institution.
- Introduces a computer-related contaminant (e.g., malicious code, virus, worm, etc.) into any IT device or network.
- Makes multiple attempts to access an IT device or network system within a brief period of time.

4.2. CYBER INTRUSION REPORTING – The budget unit shall notify SIPC within one hour of detecting the intrusion by whatever means of communication is both available and fastest (i.e., phone, fax, e-mail, courier).

- The following information, at a minimum, is required when reporting intrusions to SIPC:

  a. Budget unit name;
  b. The budget unit SIPC Coordinator's name and phone number; and
  c. Brief description of intrusion and damages (real or anticipated).

- Whenever possible, the budget unit should capture and maintain log entries for a minimum of one week following the detection of intrusion (or longer at the discretion of the application or system owner). Log entries provide significant detail that can be used for investigation and prosecution of the intruder.

4.3. SIPC INCIDENT REPORT – After notifying SIPC of the intrusion, the budget unit shall complete a SIPC Incident Report (see Attachment A) available from http://www.security.state.az.us/Security WEB Documents/CERT-WWW-IncidentReport.pdf. The budget unit representative completing the report should provide as much detail as possible in the remarks fields and annotate the description of the intrusion with explanatory remarks. As more information becomes available or the situation changes, the budget unit shall revise and re-submit the incident report to SIPC with a clear date-time stamp.

4.4. SIPC ACTIVITY – Depending on the reported damage from the intrusion, SIPC will be in constant contact with the SIPC Coordinator or designee at the affected budget unit, GITA, the Department of Public Safety, the Attorney General’s

Office, and other organizations, as necessary, until resolution and recovery efforts have been completed.

4.5. SIPC ALERT NOTIFICATIONS

4.5.1. **SIPC Responsibilities –** As SIPC creates or receives computer security alerts, it shall forward them to all budget unit CIOs or designees. Each alert shall state, as a minimum, the identity of the risk, level of risk, and any available patches or inoculants to mitigate the risk.

4.5.2. **Budget Unit Responsibilities --** Upon receiving a SIPC Alert, budget unit CIOs or designees shall notify budget unit personnel about the alert. The CIO shall send alert notifications by email and determine whether to send it to "Agency All," or specific divisions within the budget unit, or only to specific individuals, depending on the content.

4.6. SIPC MEMBERSHIP – Each budget unit shall be a member of SIPC. The budget unit CIO or designee shall complete a SIPC Membership Application (see Attachment B) and deliver it to ADOA SIPC. The budget unit CIO or designee shall ensure that the contact information on the form remains current and apprise SIPC of any changes.

5. DEFINITIONS AND ABBREVIATIONS

Refer to the PSP Glossary of Terms located on the GITA website at http://www.azgita.gov/policies_standards/ for definitions and abbreviations.

6. REFERENCES

6.1. A. R. S. § 41-621 et seq., “Purchase of Insurance; coverage; limitations, exclusions; definitions.”
6.2. A. R. S. § 41-1335 ((A (6 & 7))),“State Agency Information.”
6.3. A. R. S. § 41-1339 (A),“Depository of State Archives.”
6.4. A. R. S. § 41-1461, “Definitions.”
6.5. A. R. S. § 41-1463, “Discrimination; unlawful practices; definition.”
6.6. A. R. S. § 41-1492 et seq., “Prohibition of Discrimination by Public Entities.”
6.7. A. R. S. § 41-2501 et seq., “Arizona Procurement Codes, Applicability.”
6.8. A. R. S. § 41-3501, “Definitions.”
6.9. A. R. S. § 41-3504, “Powers and Duties of the Agency.”
6.10. A. R. S. § 41-3521, “Information Technology Authorization Committee; members; terms; duties; compensation; definition.”
6.11. A. R. S. § 44-7041, “Governmental Electronic Records.”
6.12. Arizona Administrative Code, Title 2, Chapter 7, “Department of Administration Finance Division, Purchasing Office.”
6.13. Arizona Administrative Code, Title 2, Chapter 10, “Department of Administration Risk Management Section.”
6.14. Arizona Administrative Code, Title 2, Chapter 18, “Government Information Technology Agency.”

6.15. Statewide Policy P100, Information Technology.
6.16. Statewide Policy P800, IT Security.
6.17. State of Arizona Target Security Architecture, http://www.azgita.gov/enterprise_architecture.

7. ATTACHMENTS

Attachment A – Incident Response Report
Attachment B – ADOA SIPC Membership Application

Attachment A – Incident Response Report

World Wide Web

Computer Emergency Response Team

Incident Report

Agency: **Date:**

Contact Name: **Phone:**

Email: **Fax:**

Virus/Intrusion Name:

Date of Incident: **Time of Incident:**

1. **Describe how the intrusion was discovered, its problems, systems affected, and damages:**

2. **Describe possible solutions for resolving the problems:**

3. **Describe recovery methods of system, information, data, networks, etc.:**

4. **Estimated date and time system will be available to users/customers:**

5. **Location of Computer System:**

6. **Is the affected system/network critical to the mission of the agency?** □ Yes □ No

7. **Is there evidence of spoofing?** □ Yes □ No □ Unknown

8. **Who is the anti-virus provider for the agency?**

9. **List the apparent source of the intrusion/attack (IP address), if known:**

10. **The last time the operating system was updated?**

11. **Please check type of problems and damages that apply:**

	□	Trojan Horse	□	Unauthorized Root Access	□	Network Damages
	□	Trapdoor	□	Web Site Defacement	□	Information/Data Damages
	□	Bomb	□	Denial of Service	□	Theft of Information/Data
	□	Worm	□	Distributed Denial of Service	□	Network Damages
	□	Hoax	□	Operating System Damages	□	Other, please describe:

12. **Suspected perpetrator or possible motivation of attack:**

	□	Insider/Disgruntled Employee	□	Former Employee	□	Domestic Perpetrator
	□	International perpetrator	□	Other, please describe:		

13. What operating software systems were affected?						
	□	UNIX	□	Sun OS/Solaris	□	OS2
	□	LINUX	□	MacOS	□	Windows
	□	NT	□	Sun OS/Solaris	□	Other, Please describe:
14. What Hardware systems were affected?						
	□	Compaq	□	Packard Bell	□	Toshiba
	□	Dell	□	Apple	□	Micron
	□	HP	□	Gateway	□	PC Clone
	□	IBM	□	Fujitsu	□	Other, please describe:
15. CPU/Speed:						
	□	Pentium/90	□	Pentium/233	□	Pentium/400
	□	Pentium/100	□	Pentium/300	□	Pentium/450
	□	Pentium/133	□	Pentium/333	□	Motorola
	□	Pentium/200	□	Pentium/350	□	Other, please describe:
16. Memory:						
	□	16 MB	□	32 MB	□	64 MB
	□	128 MB	□	Other, please describe:		
17. Modem Speed:						
	□	28.8 baud	□	33.6 Baud	□	56 Baud
	□	ISDN	□	Other, please describe:		
18. Internet Browser:						
	□	Microsoft Internet Explorer	□	Netscape Navigator/Communicator	□	Other, please describe:
19. Agency Security Infrastructure (check all that apply):						
	□	CERT Team	□	Security Auditing Tool(s)	□	Secure Remote Access Tools
	□	Firewall(s)	□	Packet Filtering	□	Banners
	□	Intrusion Detection System(s)	□	Encryption	□	Account/Access Control List
	□	Other, please describe:				
20. What actions and technical mitigation have been taken?						
	□	System disconnected from network	□	System binaries checked	□	No action taken
	□	Backup of affected system(s)	□	Log files examined	□	Other, Please describe:

21. Critical State services affected (check all that apply):

	□	Health	□	Transportation	□	Criminal Justice
	□	Public Safety	□	Agriculture	□	Education/Higher Ed.
	□	Corrections	□	Labor Employment	□	Revenue
	□	Environmental	□	Human/Social Services	☒	Administration

22. Please list other agency/organization that been informed? (Please provide names and phone numbers)

	□	DPS	□	State SIPC
	□	Attorney General	□	State CERT
	□	Other, please describe:		

Attachment B – ADOA SIPC Membership Application

JANET NAPOLITANO
GOVERNOR

BETSEY BAYLESS
DIRECTOR

ARIZONA DEPARTMENT OF ADMINISTRATION
INFORMATION SERVICES DIVISION
100 N 15th AVE., SUITE 400
PHOENIX, ARIZONA 85007

MEMORANDUM

TO: **Lee Lane, Statewide Security Manager**
ADOA ISD Security Services

SUBJECT: **Membership to the State Infrastructure Protection Center (SIPC) Alert Group**

This membership requires personal contact information in the event of an incident or alert on a vulnerability exists that may or may not directly affect your organization.

Name:	
Agency Name:	
Address:	
City:	
Telephone Number:	
Pager Number:	
FAX Number:	
Email:	

Send to Lee Lane, ADOA/ISD Security Services, 100 N 15th Ave., Suite 400, Phoenix, AZ 85007 or FAX 602-542-0095